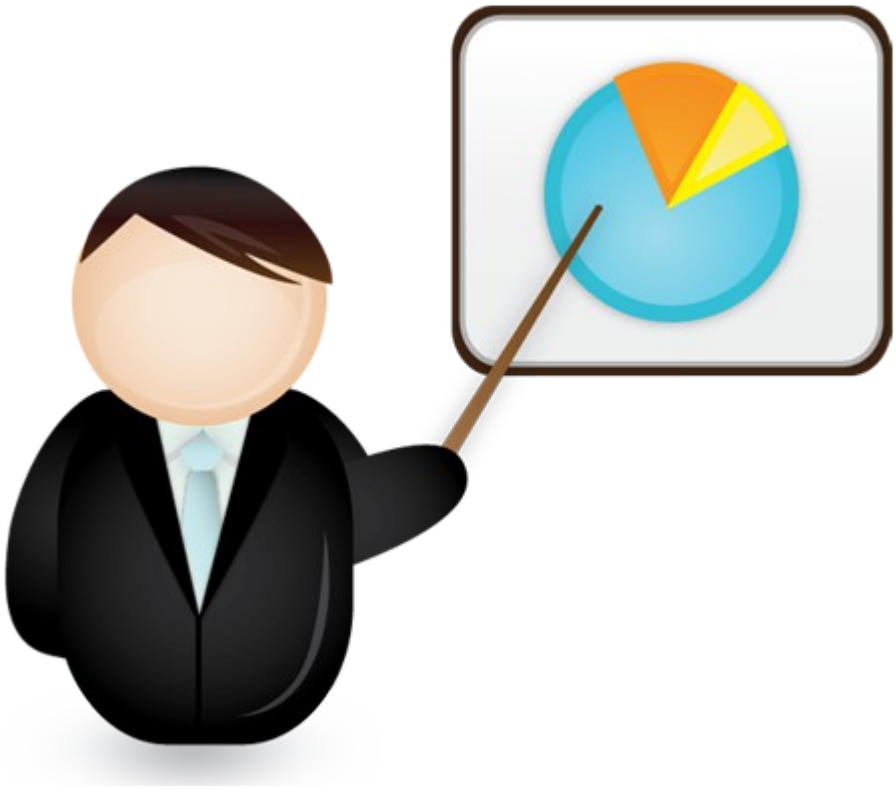
Speghiamo “l'internet” a chi era assente



piccolo vocabolario per chi si è perso qualche puntata
e parla (e spesso scrive) a sproposito

Troll
Hacker
Fake
NewsGroup
Irc
ICQ
BotNet
DdoS
Meme
4Chan
Chanology

...spiegati ai giovani (e neofiti) che fanno i tuttologi della rete

Troll

Di norma l'obiettivo di un troll è far perdere la pazienza agli altri utenti, spingendoli a insultare e aggredire a loro volta (generando una flame war). Una tecnica comune del troll consiste nel prendere posizione in modo plateale, superficiale e arrogante su una questione vissuta come sensibile e già lungamente dibattuta degli altri membri della comunità (per esempio una religion war). In altri casi, il troll interviene in modo apparentemente insensato o volutamente ingenuo, con lo scopo di irridere quegli utenti che, non capendone gli obiettivi, si sforzano di rispondere a tono ingenerando ulteriore discussione e senza giungere ad alcuna conclusione concreta.
Il cross posting, ovvero la pubblicazione di un messaggio in più sezioni diverse, è un sistema utilizzato dal troll per infastidire più gruppi contemporaneamente.
Un troll particolarmente tenace ed astuto può scoraggiare gli utenti di una comunità virtuale fino a causarne la chiusura.
La figura del troll può coincidere in alcuni aspetti con quella del fake, ovvero colui che disturba una comunità fingendosi qualcun altro. Tuttavia, un fake potrebbe partecipare in modo disciplinato e costruttivo alla conversazione (diversamente dal troll), mentre un troll potrebbe non celare né falsificare la propria identità (diversamente dal fake). Sovente le due figure, però, hanno obiettivi sovrapponibili.
I primi riferimenti all'uso del termine "troll" sono presenti nell'archivio Usenet e risalgono agli anni ottanta. Non è tuttavia chiaro se il significato attribuito al termine fosse quello successivamente attribuitogli o se fosse un semplice epiteto utilizzato fra i vari possibili.
L'origine più probabile del termine troll è nella frase "trolling for newbies", che divenne popolare nei primi anni 1990 nel gruppo Usenet alt.folklore.urban: un detto scherzoso fra utenti di lunga data che presentavano domande o argomenti tanto ripetuti e dibattuti che solamente un nuovo utente poteva perder tempo a rispondervi. Altri estesero il significato per includere il comportamento di utenti disinformati; tuttavia i troll erano ancora considerati nell'accezione ironica, più che provocatrice.

Secondo vari studi, sebbene comportamenti di disturbo siano riscontrabili anche nelle normali relazioni interpersonali, un ruolo chiave che spinge ad agire come troll nelle comunità virtuali è la sensazione di anonimato che molti utenti percepiscono durante la navigazione su internet.
Poiché la definizione stessa di troll non è condivisa, cosa spinga un utente ad agire come tale è oggetto di dibattito. Alcune motivazioni:

- Ricerca di attenzione: dominare la discussione incitando l'astio e dirottando efficacemente l'attenzione verso di sé.
- Divertimento o satira: irridere chi si infervora seriamente e perde tempo per le parole volutamente provocatorie di un totale sconosciuto, provocando grandi discussioni con poca fatica.
- Disagio personale: reazione a situazioni di disagio familiare, scolastico, finanziario o relazionale; per esempio combattendo sentimenti di inferiorità attraverso l'esperienza di controllare un ambiente.
- Ragioni economiche: sfruttare la figura dei troll come mezzo di marketing per attrarre utenti e discussioni in una comunità o far parlare di sé.
- Modificare l'opinione: ostentare opinioni estreme per fare in modo che le proprie vere opinioni, poi, sembrino moderate, e convincere quindi un gruppo di utenti a seguirle.
- Combattere il conformismo: rompere la chiusura e il conformismo del gruppo agendo con una "terapia d'urto".
- Attaccare un utente o un gruppo: agire personalmente contro un soggetto o gruppo di soggetti per ripicca, gelosia, non condivisione di idee o altra ragione.
- Diminuire il rapporto segnale/rumore: diluire i messaggi informativi in un fiume di messaggi inutili, per far perdere interesse e utilità al gruppo o all'argomento discusso.
- Verificare la robustezza di un sistema: violare le regole e i termini d'uso per controllare se e

come gli amministratori/moderatori prendono contromisure.

- Ricerca sociologica: studiare il fenomeno per ragioni di ricerca sociologico/scientifica.

Nelle comunità virtuali, alcuni utenti agiscono come "cacciatori di troll", entrando volontariamente in conflitto con altri utenti che reputano tali e finendo per essere a loro volta dannosi per la comunità (dando, per l'appunto, "da mangiare al troll").
Durante i conflitti causati dai troll il comportamento degli utenti si può dividere in categorie:

- Il Troll: chi attivamente fomenta gli scontri e gli attriti (volontariamente o involontariamente).
- I Dirottatori o Foraggiatori: coloro che rispondono animatamente ai messaggi provocatori del troll, "dandogli da mangiare".
- Il Cacciatore di troll: che non inizia il conflitto, ma se coinvolto ricambia con eguale protervia, talvolta sfruttando il troll stesso per agire in modo aggressivo e accusando quindi spesso falsi positivi.
- Il Nobile: chi cerca di ignorare il conflitto, continuando a discutere gli altri argomenti; esprimendo disapprovazione per il troll ma non sfidandolo, postando consigli semplici ed efficaci del tipo "non date da mangiare ai troll" o altre frasi volte alla pacatezza o all'ironia gentile ("suvvia, ragazzi, ignoratelo e se ne andrà da solo").
- I Moderanti o Moderatori: chi cerca di risolvere attivamente il conflitto in modo che tutte le parti in causa restino il più possibile soddisfatte, dando talvolta involontariamente "da mangiare ai troll".
- Gli Spettatori: chi si allontana dal conflitto limitandosi a osservare o anche abbandonando la comunità.

Sebbene il "troll" sia generalmente considerato una presenza indesiderabile, la sua attività può in taluni casi portare conseguenze utili alla comunità. Esso può infatti:

- rafforzare il sistema contro gli attacchi e contribuire a formare i soggetti che si occupano della prevenzione.
- contribuire alla maturazione democratica di una comunità nel tollerare il dissenso.
- scardinare posizioni di potere, dominanti o di controllo autoritario all'interno di una comunità.
- stimolare o rianimare, anche involontariamente, le discussioni e la partecipazione informativa.
- rivelare la presenza di altri troll nascosti o l'abuso da parte di amministratori e moderatori dei propri poteri di controllo.

Hacker

Un hacker (termine coniato negli Stati Uniti d'America che si può rendere in italiano con pirata informatico) è una persona che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte, non limitatamente ai suoi ambiti d'interesse (che di solito comprendono l'informatica o l'ingegneria elettronica), ma in tutti gli aspetti della sua vita.
Esiste un luogo comune, usato soprattutto dai mass media (a partire dagli anni ottanta), per cui il termine hacker viene associato ai criminali informatici, la cui definizione corretta è, invece, "cracker".

Il New Hacker Dictionary, compendio online dove sono raccolti i termini gergali dei programmatori, elenca ufficialmente nove diverse connotazioni per la parola "hack" e un numero analogo per "hacker". Eppure la stessa pubblicazione include un saggio d'accompagnamento in cui si cita Phil Agre, un hacker del Massachusetts Institute of Technology (MIT) che mette in guardia i lettori a non farsi fuorviare dall'apparente flessibilità del termine. "Hack ha solo un significato" - sostiene Agre - "Quello estremamente sottile e profondo di qualcosa che rifiuta ulteriori spiegazioni."

A prescindere dall'ampiezza della definizione, la maggioranza degli odierni hacker ne fa risalire l'etimologia al MIT, dove il termine fece la sua comparsa nel gergo studentesco all'inizio degli anni cinquanta. Secondo una pubblicazione diffusa nel 1990 dal MIT Museum, a documentare il fenomeno dell'hacking, per quanti frequentavano l'istituto in quegli anni il termine "hack" veniva usato con un significato analogo a quello dell'odierno "goof" (scemenza, goliardata). Stendere una vecchia carcassa fuori dalla finestra del dormitorio veniva considerato un "hack", ma altre azioni più pesanti o dolose - ad esempio, tirare delle uova contro le finestre del dormitorio rivale, oppure deturpare una statua nel campus - superavano quei limiti. Era implicito nella definizione di "hack" lo spirito di un divertimento creativo e innocuo.

È a tale spirito che s'ispirava il gerundio del termine: "hacking". Uno studente degli anni cinquanta che trascorreva gran parte del pomeriggio chiacchierando al telefono o smontando una radio, poteva descrivere quelle attività come "hacking". Di nuovo, l'equivalente moderno per indicare le stesse attività potrebbe essere la forma verbale derivata da "goof" - "goofing" o "goofing off" (prendere in giro qualcuno, divertirsi).

Più avanti negli anni cinquanta, il termine "hack" acquistò una connotazione più netta e ribelle. Al MIT degli anni cinquanta vigeva un elevato livello di competizione e l'attività di hacking emerse sia come reazione sia come estensione di una tale cultura competitiva. Goliardate e burle varie divennero tutt'a un tratto un modo per scaricare la tensione accumulata, per prendere in giro l'amministrazione del campus, per dare spazio a quei pensieri e comportamenti creativi repressi dal rigoroso percorso di studio dell'istituto. Va poi aggiunto che quest'ultimo, con la miriade di corridoi e tunnel sotterranei, offriva ampie opportunità esplorative per quegli studenti che non si facevano intimorire da porte chiuse e da cartelli tipo "Vietato l'ingresso". Fu così che "tunnel hacking" divenne l'accezione usata dagli stessi studenti per indicare queste incursioni sotterranee non autorizzate. In superficie il sistema telefonico del campus offriva analoghe opportunità. Grazie ad esperimenti casuali ma accurati, gli studenti impararono a fare scherzi divertenti. Traendo ispirazione dal più tradizionale "tunnel hacking", questa nuova attività venne presto battezzata "phone hacking", per poi diventare l'odierno phreaking.
La combinazione tra divertimento creativo ed esplorazioni senza limiti costituirà la base per le future mutazioni del termine hacking. I primi ad auto-qualificarsi "computer hacker" nel campus del MIT negli anni sessanta traevano origine da un gruppo di studenti appassionati di modellismo ferroviario, che negli ultimi anni cinquanta si erano riuniti nel Tech Model Railroad Club. Una

ristretta enclave all'interno di quest'ultimo era il comitato Signals and Power (segnali ed elettricità) - gli addetti alla gestione del sistema del circuito elettrico dei trenini del club. Un sistema costituito da un sofisticato assortimento di relè e interruttori analogo a quello che regolava il sistema telefonico del campus. Per gestirlo era sufficiente che un membro del gruppo inviasse semplicemente i vari comandi tramite un telefono collegato al sistema, osservando poi il comportamento dei trenini.

I nuovi ingegneri elettrici responsabili per la costruzione e il mantenimento di tale sistema considerarono lo spirito di simili attività analogo a quello del phone hacking. Adottando il termine hacking, iniziarono così a raffinarne ulteriormente la portata. Dal punto di vista del comitato Signals and Power, usare un relè in meno in un determinato tratto di binari significava poterlo utilizzare per qualche progetto futuro. In maniera sottile, il terminehacking si trasformò da sinonimo di gioco ozioso, a un gioco in grado di migliorare le prestazioni o l'efficienza complessiva del sistema ferroviario del club. Quanto prima i membri di quel comitato cominciarono a indicare con orgoglio l'attività di ricostruzione e miglioramento del circuito per il funzionamento delle rotaie con il termine "hacking", mentre "hacker" erano quanti si dedicavano a tali attività.
Considerata la loro affinità per i sistemi elettronici sofisticati - per non parlare della tradizionale avversione degli studenti del MIT verso porte chiuse e divieti d'ingresso - non ci volle molto prima che gli hacker mettessero le mani su una macchina appena arrivata al campus. Noto come TX-0, si trattava di uno dei primi modelli di computer lanciati sul mercato. Sul finire degli anni cinquanta, l'intero comitato Signals and Power era emigrato in massa nella sala di controllo del TX-0, portandosi dietro lo stesso spirito di gioco creativo. Il vasto reame della programmazione informatica avrebbe portato a un ulteriore mutamento etimologico. "To hack" non indicava più l'attività di saldare circuiti dalle strane sembianze, bensì quella di comporre insieme vari programmi, con poco rispetto per quei metodi o procedure usati nella scrittura del software "ufficiale". Significava inoltre migliorare l'efficienza e la velocità del software già esistente che tendeva a ingolfare le risorse della macchina. Ed è qui che successivamente si colloca una diversa radice del termine hacker, la forma sostantiva del verbo inglese "to hack" che significa "tagliare", "sfrondare", "sminuzzare", "ridurre", "aprirsi un varco", appunto fra le righe di codice che istruiscono i programmi software. Un hacker era quindi uno che riduceva la complessità e la lunghezza del codice sorgente, con un "hack", appunto, una procedura grossolana ma efficace, che potrebbe essere tradotta in italiano come "zappata" o "accettata" (tagliata con l'accetta) o altrimenti con una "furbata". Rimanendo fedele alla sua radice, il termine indicava anche la realizzazione di programmi aventi l'unico scopo di divertire o di intrattenere l'utente, come "scrivere numeri romani" (cit. Richard Stallman).

Un classico esempio di quest'ampliamento della definizione di hacker è *Spacewar!,* il primo video game interattivo. Sviluppato nei primi anni sessantadagli hacker del MIT, Spacewar! includeva tutte le caratteristiche dell'hacking tradizionale: era divertente e casuale, non serviva ad altro che a fornire una distrazione serale alle decine di hacker che si divertivano a giocarvi. Dal punto di vista del software, però, rappresentava una testimonianza incredibile delle innovazioni rese possibili dalle capacità di programmazione. Inoltre era completamente libero (e gratuito). Avendolo realizzato per puro divertimento, gli hacker non vedevano alcun motivo di mettere sotto scorta la loro creazione, che finì per essere ampiamente condivisa con altri programmatori. Verso la fine degli anni sessanta, Spacewar! divenne così il passatempo preferito di quanti lavoravano ai mainframe in ogni parte del mondo.

Furono i concetti di innovazione collettiva e proprietà condivisa del software a distanziare l'attività di computer hacking degli anni sessanta da quelle di tunnel hacking e phone hacking del decennio precedente. Queste ultime tendevano a rivelarsi attività condotte da soli o in piccoli gruppi, per lo più limitate all'ambito del campus, e la natura segreta di tali attività non favoriva l'aperta circolazione di nuove scoperte. Invece i computer hacker operavano all'interno di una disciplina

scientifica basata sulla collaborazione e sull'aperto riconoscimento dell'innovazione. Non sempre hacker e ricercatori "ufficiali" andavano a braccetto, ma nella rapida evoluzione di quell'ambito le due specie di programmatori finirono per impostare un rapporto basato sulla collaborazione - si potrebbe perfino definire una relazione simbiotica.
Il fatto che la successiva generazione di programmatori, incluso Richard Stallman, aspirasse a seguire le orme dei primi hacker, non fa altro che testimoniare le prodigiose capacità di questi ultimi. Nella seconda metà degli anni settanta il termine "hacker" aveva assunto la connotazione di élite. In senso generale, computer hacker era chiunque scrivesse il codice software per il solo gusto di riuscirci. In senso specifico, indicava abilità nella programmazione. Al pari del termine "artista", il significato conteneva delle connotazioni tribali. Definire hacker un collega programmatore costituiva un segno di rispetto. Auto-descriversi come hacker rivelava un'enorme fiducia personale. In entrambi i casi, la genericità iniziale dell'appellativo computer hacker andava diminuendo di pari passo alla maggiore diffusione del computer.

Con il restringimento della definizione, l'attività di computer hacking acquistò nuove connotazioni semantiche. Per potersi definire hacker, una persona doveva compiere qualcosa di più che scrivere programmi interessanti; doveva far parte dell'omonima cultura e onorarne le tradizioni allo stesso modo in cui un contadino del Medio Evo giurava fedeltà alla corporazione dei vinai. Pur se con una struttura sociale non così rigida come in quest'ultimo esempio, gli hacker di istituzioni elitarie come il MIT, Stanford e Carnegie Mellon iniziarono a parlare apertamente di "etica hacker": le norme non ancora scritte che governavano il comportamento quotidiano dell'hacker. Nel libro del 1984 "Hackers. Gli eroi della rivoluzione informatica", l'autore Steven Levy, dopo un lungo lavoro di ricerca e consultazione, codificò tale etica in cinque principi fondamentali.

Sotto molti punti di vista, i principi elencati da Levy continuano a definire l'odierna cultura del computer hacking. Eppure l'immagine di una comunità hacker analoga a una corporazione medievale, è stata scalzata dalle tendenze eccessivamente populiste dell'industria del software. A partire dai primi anni ottanta i computer presero a spuntare un po' ovunque, e i programmatori che una volta dovevano recarsi presso grandi istituzioni o aziende soltanto per aver accesso alla macchina, improvvisamente si trovarono a stretto contatto con hacker di grande livello via ARPANET. Grazie a questa vicinanza, i comuni programmatori presero ad appropriarsi delle filosofie anarchiche tipiche della cultura hacker di ambiti come quello del MIT. Tuttavia, nel corso di un simile trasferimento di valori andò perduto il tabù culturale originato al MIT contro ogni comportamento malevolo, doloso. Mentre i programmatori più giovani iniziavano a sperimentare le proprie capacità con finalità dannose - creando e disseminando virus, facendo irruzione nei sistemi informatici militari, provocando deliberatamente il blocco di macchine quali lo stesso Oz del MIT, popolare nodo di collegamento con ARPAnet - il termine "hacker" assunse connotati punk, nichilisti. Quando polizia e imprenditori iniziarono a far risalire quei crimini a un pugno di programmatori rinnegati che citavano a propria difesa frasi di comodo tratte dall'etica hacker, quest'ultimo termine prese ad apparire su quotidiani e riviste in articoli di taglio negativo. Nonostante libri come quello di Levy avessero fatto parecchio per documentare lo spirito originale di esplorazione da cui nacque la cultura dell'hacking, per la maggioranza dei giornalisti "computer hacker" divenne sinonimo di "rapinatore elettronico". Contro l'originale definizione da questo momento si insinua nella conoscenza popolare l'uguaglianza Hacker-Malvivente.

Anche di fronte alla presenza, durante gli ultimi due decenni, delle forti lamentele degli stessi hacker contro questi presunti abusi, le valenze ribelli del termine risalenti agli anni cinquanta rendono difficile distinguere tra un quindicenne che scrive programmi capaci di infrangere le attuali protezioni cifrate, dallo studente degli anni sessanta che rompe i lucchetti e sfonda le porte per avere accesso a un terminale chiuso in qualche ufficio. D'altra parte, la sovversione creativa dell'autorità per qualcuno non è altro che un problema di sicurezza per qualcun altro. In ogni caso, l'essenziale tabù contro comportamenti dolosi o deliberatamente dannosi trova conferma a tal punto

da spingere la maggioranza degli hacker ad utilizzare il termine cracker - qualcuno che volontariamente decide di infrangere un sistema di sicurezza informatico per rubare o manomettere dei dati - per indicare quegli hacker che abusano delle proprie capacità.
Questo fondamentale tabù contro gli atti dolosi rimane il primario collegamento culturale esistente tra l'idea di hacking del primo scorcio del XXI secolo e quello degli anni cinquanta. È importante notare come, mentre la definizione di computer hacking abbia subìto un'evoluzione durante gli ultimi quattro decenni, il concetto originario di hacking in generale - ad esempio, burlarsi di qualcuno oppure esplorare tunnel sotterranei - sia invece rimasto inalterato. Nell'autunno 2000 il MIT Museum onorò quest'antica tradizione dedicando al tema un'apposita mostra, la Hall of Hacks. Questa comprendeva alcune fotografie risalenti agli anni venti, inclusa una in cui appare una finta auto della polizia. Nel 1993, gli studenti resero un tributo all'idea originale di hacking del MIT posizionando la stessa macchina della polizia, con le luci lampeggianti, sulla sommità del principale edificio dell'istituto. La targa della macchina era IHTFP, acronimo dai diversi significati e molto diffuso al MIT e attualmente la stessa macchina è esposta all'interno dell'edificio del MIT, Ray and Maria Stata Center. La versione maggiormente degna di nota, anch'essa risalente al periodo di alta competitività nella vita studentesca degli anni cinquanta, è "I hate this fucking place" (Odio questo fottuto posto). Tuttavia nel 1990, il Museum riprese il medesimo acronimo come punto di partenza per una pubblicazione sulla storia dell'hacking. Sotto il titolo "Institute for Hacks Tomfoolery and Pranks" (Istituto per scherzi folli e goliardate), la rivista offre un adeguato riassunto di quelle attività.
"Nella cultura dell'hacking, ogni creazione semplice ed elegante riceve un'alta valutazione come si trattasse di scienza pura", scrive Randolph Ryan, giornalista del Boston Globe, in un articolo del 1993 incluso nella mostra in cui compariva la macchina della polizia. "L'azione di hack differisce da una comune goliardata perché richiede attenta pianificazione, organizzazione e finezza, oltre a fondarsi su una buona dose di arguzia e inventiva. La norma non scritta vuole che ogni hack sia divertente, non distruttivo e non rechi danno. Anzi, talvolta gli stessi hacker aiutano nell'opera di smantellamento dei propri manufatti".

A questo proposito all'ingresso del MIT Ray and Maria Stata Center è presente un cartello intitolato "Hacking Ethics" che riporta 11 punti a cui dovrebbe rifarsi ogni hacker. Questi sono:

1. Be safe. Your safety, the safety of your fellow jackers, and the safety of anyone you hack should never be compromised.
2. Be subtle. Leave no evidence that you were ever there.
3. Leave things as you found them (or better).
4. If you find something broken, call F-IXIT (the local number for reporting problems wit the buildings and grounds). Hackers often go places that institute workers do not frequent regularly and may see problems before anyone else.
5. Leave no damage.
6. Do not steal anything.
7. Brute force is the last resort of the incompetent. ("One who breaks a thing to find out what it is has left the path of reason." - John Ronald Reuel Tolkien, "The Lord of the Rings")
8. Do not hack while under the influence of alcohol/drugs/etc.
9. Do not drop things (off a building) without ground crew.
10. Do not hack alone (just like swimming).
11. Above all, exercise common sense.

Inoltre, sempre all'ingresso del MIT, è presente un altro cimelio della storia dell'hacking proprio accanto ai "comandamenti" dell'etica di un Hacker: L'idrante del MIT collegato a una fontana indicante la famosa frase del presidente del MIT Jerome Weisner (1971-1980) "Getting an education at MIT is like taking a drink from a fire hose", ovvero, "Essere istruiti al MIT è come bere da un tubo antincendio".

Il desiderio di confinare la cultura del computer hacking all'interno degli stessi confini etici appare opera meritevole ma impossibile. Nonostante la gran parte dell'hacking informatico aspiri al medesimo spirito di eleganza e semplicità, il medium stesso del software offre un livello inferiore di reversibilità. Smontare una macchina della polizia è opera semplice in confronto allo smantellamento di un'idea, soprattutto quando è ormai giunta l'ora per l'affermazione di tale idea. Da qui la crescente distinzione tra "black hat" e "white hat" ("cappello nero" e "cappello bianco") - hacker che rivolgono nuove idee verso finalità distruttive, dolose contro hacker che invece mirano a scopi positivi o, quantomeno, informativi.
Una volta oscuro elemento del gergo studentesco, la parola "hacker" è divenuta una palla da biliardo linguistica, soggetta a spinte politiche e sfumature etiche. Forse è questo il motivo per cui a così tanti hacker e giornalisti piace farne uso. Nessuno può tuttavia indovinare quale sarà la prossima sponda che la palla si troverà a colpire.
Un "h4x0r" (pronuncia "achs-or") è il termine hacker scritto in leet (linguaggio degli hacker).

Fake

Fake è un termine inglese, che sta a significare falso, contraffatto, alterato.
Come neologismo italiano, è stato usato per indicare la sostituzione di contenuti pubblicitari con slogan di protesta, come critica a certe politiche aziendali.
Nel gergo di Internet, e in particolare di comunità virtuali come newsgroup, forum o chat, un fake (dall'inglese per "falso", "posticcio") è un utente che falsifica in modo significativo la propria identità.

Uno degli episodi più celebri inerenti al fenomeno dei fake avvenne nel 1982-1983 sulla chat americana di CompuServe, ed è ricordato col nome "AlexAndJoan" ("Alex e Joan"). Alex (nella vita reale un riservato psichiatra cinquantenne di New York) si spacciò a lungo per una donna muta, una neuropsicologa altezzosa e antireligiosa, divenuta paraplegica in seguito ad un incidente stradale, di nome Joan. La sua spiegazione fu che il suo era un esperimento messo in atto "per poter meglio relazionarsi con le proprie pazienti".
L'impostura andò avanti per due anni e "Joan" divenne un personaggio assai dettagliato, con una complessa rete di relazioni emotive: la storia finì solo quando "Joan" coinvolse un amico conosciuto online in un incontro con Alex.
Anche quelli che conoscevano poco Joan si sentirono coinvolti (e in qualche misura traditi) dall'inganno di Alex. A molti di noi online piace pensare di essere una comunità utopica del futuro, e l'esperimento di Alex ci ha dimostrato che la tecnologia non è una difesa contro le truffe. Abbiamo perso la nostra innocenza, se non la nostra fede. (Van Gelder, 1996, p.534)

NewsGroup

Un newsgroup è uno degli spazi virtuali creato su una rete di server interconnessi (storicamente una sottorete di Internet USENIX network o più semplicemente Usenet) per discutere di un argomento (topic) ben determinato. In italiano a volte viene utilizzato il termine gruppo di discussione.
I news server comunicano fra loro (attraverso il protocollo NNTP) in modo che i messaggi inviati ad un server si trovino duplicati su tutti gli altri server. Per diversi motivi (economie di spazio, interesse degli utenti, censura), non tutti i server contengono gli stessi NewsGroup. Ogni gestore di news server (spesso gli stessi provider ISP) può decidere infatti quali NewsGroup tenere.
L'accesso a queste aree tematiche avviene per mezzo di programmi chiamati news client o newsreader (oggi a volte integrati nei programmi di posta elettronica come ad esempio Mozilla Thunderbird, SeaMonkey, Outlook Express, Sylpheed), a una sorta di "stanza delle bacheche" (news server) che raccoglie i vari NewsGroup (o in breve NG).
Per ragioni storiche, essenzialmente dovute ai costi delle connessioni dialup che molti utenti dovevano sostenere in passato, o anche per le scarse disponibilità di accesso alla rete, i newsreader sono tuttora concepiti per operare principalmente in modalità disconnessa: gli articoli scaricati in precedenza possono essere letti e le relative risposte preparate per la spedizione senza che sia necessaria una connessione attiva; la successiva connessione permette in un'unica soluzione il download degli articoli apparsi sul server nel frattempo e l'upload delle risposte. Questa modalità, nient'affatto in "tempo reale", è una caratteristica tipica del servizio che deve essere tenuta in considerazione: la netiquette dei newsgroup disapprova, ad esempio, chi sollecita risposte immediate ai propri articoli. Quando si risponde ad un messaggio, è buona cosa riportare (o come detto in gergo: quotare) parte del testo a cui si risponde, in modo da facilitarne la lettura.
Questo approccio viene in parte deviato dall'accesso on-line offerto dai portali web, che possono consentire una partecipazione attiva ai newsgroup con relativa facilità ma soprattutto sofisticati strumenti di ricerca per parola chiave nei loro archivi: in particolare il servizio fornito da GoogleGroups rappresenta la "memoria storica" di usenet, conservando praticamente ogni articolo pubblicato dalla sua nascita (da ricordare come in linea di principio non vengano archiviati gli articoli dei newsgroup binari, contenenti file e gli articoli nei quali l'autore abbia apposto il contrassegno "da non archiviare" mediante X-No-Archive). È da tenere in considerazione anche che la frequenza di aggiornamento dei gruppi sui portali web è solitamente più bassa rispetto a quella che si può ottenere con una connessione diretta a usenet.
Un vantaggio importante dei portali web è quello di consentire un accesso facilitato a fruitori con scarsa dimestichezza: il newsreader per contro risulta più efficiente ma richiede una certa esperienza per essere sfruttato al meglio. I portali web, infine, sono connessi tramite il servizio HTTP, praticamente sempre disponibile anche in presenza di proxy/firewall aziendali, al contrario del servizio NNTP/NNRP usato dai newsreader.
Di norma ciascun newsgroup ha un manifesto (charter) che aiuta a comprendere quali sono gli argomenti oggetto di discussione. La netiquette, su Usenet, sconsiglia di inviare articoli fuori tema e suggerisce di seguire per qualche tempo un newsgroup prima di iniziare a scrivere.
Sono molti i newsgroup in cui i poster abituali, ossia coloro che li seguono da più tempo e con una certa assiduità, hanno redatto delle FAQ, raccolte di risposte a domande poste di frequente, così da aiutare i newbie (nuovi arrivati, principianti) ed evitare che il newsgroup contenga sempre le stesse domande o che queste provochino reazioni irritate (flame), botta e risposta interminabili e di dubbia utilità. Talora i newsgroup sono seguiti da persone che leggono i messaggi ma non partecipano attivamente. Tali persone sono chiamate, nel gergo della rete, lurker.
I newsgroup sono generalmente raggruppati all'interno di diverse gerarchie Usenet.
Esiste anche un'altra importante suddivisione, a seconda dello status di moderazione: i newsgroup moderati sono caratterizzati da un diverso funzionamento dovuto al percorso degli articoli, che vengono inviati via mail al moderatore. Tuttavia il protocollo utilizzato non è sufficientemente robusto da garantire il corretto funzionamento e l'assenza di abusi. Può capitare che si perdano degli articoli o che esistano articoli che non sono stati approvati dal moderatore.

IRC

Internet Relay Chat (IRC) è un protocollo di messaggistica istantanea su Internet, che consente sia la comunicazione diretta fra due utenti, che il dialogo contemporaneo di interi gruppi di persone in stanze di discussione chiamate canali.
IRC è un protocollo di rete aperto che utilizza il protocollo di trasmissione TCP (Transmission Control Protocol) e opzionalmente il Transport Layer Security (TLS). Un server IRC (chiamato IRCd) è in grado di connettersi con altri server IRC formando così una vera e propria rete di comunicazione; gli utenti accedono ad essa mediante la connessione di un client ad un server. Molti server IRC non richiedono all'utente di autenticarsi, ma va comunque specificato un nickname (univoco a livello della rete IRC).
IRC è un protocollo plaintext, questo significa che è possibile (comunque con qualche inconveniente) usarlo tramite una connessione socket di tipo raw. Tuttavia non vi è modo di definire il carattere di decodifica dei messaggi e dei nickname rendendo impossibile il filtraggio di caratteri non-ASCII.
Il mezzo di comunicazione fondamentale in una sessione IRC è il "canale", un gruppo di utenti identificato da un nome, dove tutti gli appartenenti possono mandare messaggi leggibili solo dagli utenti dello stesso gruppo. Un canale IRC si crea automaticamente al primo ingresso da parte di qualsiasi utente.
I nomi dei canali appartenenti a tutta un'intera rete IRC si identificano col carattere "#" iniziale, mentre quelli locali (specifici di un server) sono identificati con il carattere "*&*" (tuttavia quest'ultimo potrebbe non essere disponibile su alcune reti). Per ovviare a problemi di desincronizzazione dei canali nel momento in cui dei server si fossero scollegati furono creati i canali "!" senza i problemi di sincronismo che però ottennero scarso successo anche per la mancanza di informazione agli utenti.
Il primo utente che entra in un canale acquisisce automaticamente dei privilegi che può poi passare a qualsiasi altro utente presente nel medesimo canale; questi utenti vengono chiamatioperatori di canale (channel operator). Vi sono anche diversi utenti con privilegi differenti e con compiti di amministrazione della rete; questi sono chiamati IRC Operator (abbreviato in IRCop, spesso erroneamente confuso in IR-Cop) o in italiano "operatori IRC". Nelle implementazioni più recenti è anche possibile registrare i canali, in modo che i diritti di accesso non vengano persi alla disconnessione dell'ultimo operatore; ove questo non sia possibile viene fatto uso di bot, programmi speciali che appaiono come normali utenti, ma che presidiano il canale e, all'uso, ri-conferiscono lo status di operatore ai proprietari.
Gli "Operatori del canale" possono impostare diverse opzioni su quel determinato canale, vedi b:IRC/Modi canale.
Gli utenti nell'ambito del canale o del server possono avere diversi attributi, vedi b:IRC/Modi utente
Le connessioni IRC sono un ghiotto obiettivo per cracker malintenzionati, in quanto, pur essendo cifrate, prendono, per loro stessa natura, lunghi periodi di tempo di connessione. È necessario pertanto assicurare a queste connessioni, una accurata politica di sicurezza in grado di proteggerle dagli attacchi di script kiddie che cercano di prenderne il controllo (IRC takeover war), magari tentando di sfruttare a proprio vantaggio un netsplit (come si dice in gergo cavalcando lo split).
La connessione IRC viene spesso utilizzata da parte degli script kiddies come "laboratorio" per provare diversi tipi di attacchi in rete, per esempio inviando pacchetti ICMP (Internet Control Message Protocol) mal formati al fine di disturbarne gli utenti (vedi anche nuke). Tuttavia, con l'entrata in scena dei Bouncer (BNC) e dei virtual host, è molto difficile per queste persone malintenzionate portare a termine un attacco, visto che questi servizi riescono a nascondere l'indirizzo IP collegato ad un nickname.
In tutto il mondo, ci sono diverse centinaia di reti IRC attive. Eseguono diverse implementazioni di server IRC, e sono amministrate da vari gruppi diOperatori IRC, ma tutti i protocolli utilizzati dagli utenti IRC presentano similitudini, per cui in tutte le reti IRC si può accedere col medesimo client senza problemi.

La differenza tra i vari network sta nella gestione delle implementazioni. IRCnet ad esempio è fedele all'implementazione storica di IRC e può essere definita la rete più anarchica poiché non prevede alcun controllo di nickname o canali. Al contrario altre reti hanno sviluppato sistemi per registrare i nickname o i canali debellando così l'uso di bot e i problemi causati da ircwar.
Come in Usenet i contenuti inviati sono immediatamente visibili da più siti e su tutti i server d'accesso, però, a differenza di usenet, non sono più cancellabili. Una traccia delle discussioni (non in chat room private) è tenuta in file di log di pubblico dominio.
IRC offre le funzionalità tipiche delle chat più evolute: possibilità di creare profili-utente con dati personali, chattare, invio di messaggi privati, scambio di file, organizzare meeting della chat.
Per individuare un'ora standard in tutto il mondo è stata scelta la convenzione UTC.

ICQ

ICQ è un programma per computer di instant messaging nel mondo, creato da Mirabilis, una compagnia start-up israeliana fondata a Tel Aviv. Il programma venne rilasciato per la prima volta nel novembre del 1996. Il nome è un gioco di parole sulla frase "I seek you" (io ti cerco).
ICQ permette di mandare messaggi istantanei (anche a utenti offline), SMS, URL, cartoline; avviare chat multi-user e giochi online, trasferire file, dà la possibilità di ricevere email tramite POP3 e di condividere una cartella remota. Alcune delle caratteristiche sono basate sull'utilizzo di plug-in aggiuntivi.
Dalle preferenze del software è stato reso possibile modificare le impostazioni di sicurezza in modo da richiedere conferma ogni qualvolta accettare un utente che voglia avviare o accedere a uno dei servizi resi disponibili dal programma.
Dal 2000 gli utenti di ICQ e AIM (AOL Instant Messenger) possono aggiungersi alla lista dei contatti reciprocamente senza dover ricorrere a un altro client.
Gli utenti di ICQ sono identificati da un numero chiamato UIN (acronimo di Unique Identification Number, Universal Internet Number o anche Unified Identification Number), distribuito in ordine di sequenza.
L'UIN viene assegnato a un utente durante la registrazione e - a differenza di altri programmi di instant messaging - esso è l'unico dato che identifica un utente e, quindi, l'unico dato immodificabile. Tutte le informazioni del profilo utente, compreso il nome visualizzato, il nome utente e l'indirizzo email, sono modificabili senza bisogno di effettuare una nuova registrazione.

BotNet

Una botnet è una rete formata da dispositivi informatici collegati ad Internet e infettati da malware, controllata da un'unica entità, il botmaster. A causa di falle nella sicurezza o per mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, i dispositivi vengono infettati da virus informatici o trojan i quali consentono ai loro creatori di controllare il sistema da remoto. I controllori della botnet possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi distribuiti del tipo distributed denial of service (DDoS) contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, in taluni casi agendo persino su commissione di organizzazioni criminali. I dispositivi che compongono la botnet sono chiamati bot (da roBOT) o zombie.

I malware creati per far parte di una botnet, non appena assunto il controllo del sistema, devono poter fornire al proprio autore i dati relativi al sistema infettato. Per fare ciò spesso sfruttano i canali IRC (Internet Relay Chat) e si connettono ad un dato canale, situato su un dato server, il quale spesso è protetto da una password per dare accesso esclusivo all'autore. Tramite il canale dichat l'autore è in grado di controllare contemporaneamente tutti i sistemi infetti collegati al canale (i quali possono essere anche decine di migliaia) e di impartire ordini a questi. Per fare un esempio, con un solo comando potrebbe far partire un attacco DDoS verso un sistema a sua scelta.
Un altro sistema utilizzato dai botmaster per controllare i bot sono le reti peer-to-peer (tra queste è compresa la rete di skype). In questo caso la rete p2p viene usata come veicolo per le informazioni che il botmaster invia ai bot.

Le botnet vengono spesso utilizzate anche per altri scopi oltre al DDoS: questi virus sono spesso programmati in modo da spiare il sistema infetto e intercettare password ed altre informazioni utili. Possono anche offrire accesso alle macchine infette tramite backdoor oppure servizi proxy che garantiscono l'anonimato in rete.
Infine un altro uso delle botnet è come proxy verso un sistema compromesso. I bot infatti spesso vengono "ripuliti" e quindi di fatto non fanno parte più della botnet. Se un pirata installa un server su una di queste macchine e ne perde il controllo il danno è grave. Una tecnica usata recentemente è quella del fastflux in cui una macchina fuori dalla botnet fa girare un finto server (per esempio per fare dello spoofing) e le macchine della botnet fungono solo da proxy verso questa macchina.

DdoS

Nella sicurezza informatica DoS, scritto con la maiuscola al primo e terzo posto, è la sigla di denial of service, letteralmente negazione del servizio. Si tratta di un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio. Oltre al senso primario di denial of service come azione deliberata ci si può riferire ad esso come azione accidentale, in seguito per esempio ad una errata configurazione,o come nel caso dell'effetto Slashdot.

Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server Web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile", quindi qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul TCP è soggetto al rischio di attacchi DoS. Inizialmente questo tipo di attacco veniva attuato da "hacker", come gesto di dissenso etico nei confronti dei siti web commerciali e delle istituzioni.
Oggi gli attacchi DoS hanno la connotazione decisamente più "criminale" di impedire agli utenti della rete l'accesso ai siti web vittime dell'attacco. Per rendere più efficace l'attacco in genere vengono utilizzati molti computer inconsapevoli, detti zombie, sui quali precedentemente è stato inoculato un programma appositamente creato per attacchi DoS e che si attiva ad un comando proveniente dal cracker creatore. Se il programma maligno si è diffuso su molti computer, può succedere che migliaia di PC violati da un cracker, ovvero una botnet, producano inconsapevolmente e nello stesso istante un flusso incontenibile di dati che travolgeranno come una valanga anche i link più capienti del sito bersaglio.
Non solo i sistemi server possono essere vittime di un attacco DoS ma anche semplici utenti e client, sebbene questi attacchi siano molto meno frequenti e di nessun interesse per i cosiddetticracker.
La probabilità sempre minore di incontrare sistemi veramente vulnerabili ha fatto sì che siano diminuiti gli attacchi DoS più eclatanti, però si è scoperta un'estrema vulnerabilità della rete per l'aumento costante della potenza operativa degli attuali personal computer e dell'accesso ad Internet tramite i sistemi DNS.
L'implementazione del protocollo TCP/IP, che non garantisce particolare sicurezza sull'identificazione dei mittenti di pacchetti ma anzi ne protegge l'anonimato, può essere sfruttata per mascherarne la vera provenienza.
Trattandosi di connessioni apparentemente legittime, è impossibile bloccarle senza interrompere anche il flusso realmente inoffensivo. Però limitando drasticamente il numero di sessioni aperte simultaneamente l'impatto dell'attacco si riduce considerevolmente senza limitare il flusso dei pacchetti regolari.
Anche limitando il discorso al blocco di un sito web, esistono, e sono stati utilizzati, parecchi modi di ottenere questo risultato.

Una variante di tale approccio è il DDoS (Distributed Denial of Service) dal funzionamento identico ma realizzato utilizzando numerose macchine attaccanti che insieme costituiscono unabotnet.
Gli attaccanti tendono a non esporsi direttamente, dato che per le forze dell'ordine sarebbe relativamente semplice risalire ai computer utilizzati per l'attacco. Gli attaccanti, per evitare di essere individuati e per avere a disposizione un numero sufficiente di computer per l'attacco, infettano precedentemente un numero elevato di computer con dei virus o worm che lasciano aperte dellebackdoor a loro riservate. I computer che sono controllati dall'attaccante vengono chiamati zombie.
Tutti i computer infettati entrano a far parte di una botnet, a libera disposizione dell'attaccante: una nota interessante è data dalla distinzione tra le macchine che eseguono un Sistema OperativoWindows (definiti, in gergo, rxbot) e quelle che invece eseguono un sistema Unix, particolarmente adatte all'UDP Flooding (Flooding sul protocollo UDP).

Una particolarità degli zombies Windows è data dalla possibilità, per l'attaccante, di programmare un trojan in grado di diffondersi automaticamente a tutta una serie di contatti presenti sul computer infettato (definita, in gergo, funzione di auto-spreading): contatti contenuti nella rubrica degli indirizzi e nei contatti di programmi di Instant Messaging, come Microsoft Messenger, permettendo così al computer zombie di infettare, in maniera completamente autonoma, altre macchine che, a loro volta, diverranno parte della botnet dell'attaccante.

Quando il numero di zombies è ritenuto adeguato, o quando viene a verificarsi una data condizione, i computer infetti si attivano e sommergono il server bersaglio di richieste di connessione. Con l'avvento della banda larga il fenomeno dei DDOS sta assumendo proporzioni preoccupanti, dato che attualmente esistono milioni di persone dotate di una connessione ad Internet molto veloce e permanente ma con scarse o nulle conoscenze e contromisure riguardanti la sicurezza informatica.
Il danno maggiore dell'attacco di tipo DDoS è dovuto principalmente alla "asimmetria" che si viene a creare tra "la" richiesta e le risposte correlate in una sessione DNS (Domain Name System). Il flusso enorme di risposte generato provocheranno nel sistema una tale "inondazione" di traffico rendendo il server inadeguato alla gestione delle abituali funzioni on-line.
Inoltrando, al Sito preso di mira, una risposta di alcuni Kilobyte, per ogni richiesta contenente solo pochi bytes, si ottiene un'amplificazione esponenziale tale da saturare i canali dati più capienti, raggiungendo con il DDoS livelli finora inattuabili con gli altri tipi di attacco DoS.
Le configurazioni predefinite, standard e quelle "consigliate" di Firewall si rivelano utili a contrastare solo gli "attacchi" sferrati dall'esterno, ad esempio di un'azienda, ma poiché il traffico in Retegestito tramite sistema DNS è vitale, per fronteggiare questo tipo di attacco non si potranno attuare le stesse strategie impiegate nei confronti degli attacchi ai Ping.
Quindi il Network manager dovrà tenere scrupolosamente sotto controllo e monitoraggio i canali di flusso dati e, per escludere l'intervento o contrastare l'azione di un cracker, riconfigurerà il DNS responsabile del sito.

Una particolare categoria di DDoS è il cosiddetto Distributed Reflection Denial of Service (DRDoS). In questa particolare tipologia di attacco, il computer attaccante produce delle richieste di connessione verso server con connessioni di rete molto veloci utilizzando come indirizzo di provenienza non il proprio bensì quello del bersaglio dell'attacco. In questo modo i server risponderanno affermativamente alla richiesta di connessione non all'attaccante ma al bersaglio dell'attacco. Grazie all'effetto moltiplicatore dato dalle ritrasmissioni dei server contattati, che a fronte della mancanza di risposta da parte del bersaglio dell'attacco (apparentemente l'iniziatore della connessione) provvederanno a ritrasmettere (fino a 3 volte solitamente) il pacchetto immaginandolo disperso, entrando così in un circolo vizioso che vede rapidamente esaurirsi le risorse del bersaglio.
Quest'ultimo tipo di attacco è particolarmente subdolo perché, a causa della natura delle risposte, è difficilmente schermabile dall'utente comune: infatti se si filtrassero le risposte dei server verrebbe compromessa la funzionalità stessa della connessione di rete impedendo, di fatto, la ricezione anche delle informazioni desiderate. Le risposte dei server, sollecitate dall'attaccante, sono infatti indistinguibili da quelle generate da una richiesta legittima della vittima. Il problema si sta presentando con maggiore incidenza da quando Microsoft ha deciso di rendere le "Raw Sockets", interfaccia di accesso al TCP/IP, facilmente disponibili. Le RAW sockets permettono appunto di cambiare l'indirizzo di provenienza del pacchetto per sostituirlo con quello della vittima, fatto che è strumentale per questo tipo di attacco.

MeMe

Un fenomeno di Internet (o Internet meme) si ha quando qualcosa diventa improvvisamente celebre tramite la propagazione di informazioni attraverso la rete Internet.
L'assenza di confini fisici della rete tende a favorire una rapida diffusione di idee e novità, specialmente se queste hanno contenuti umoristici o bizzarri. In molti casi, proprio se il motivo della diffusione è essenzialmente goliardico, la cosa di cui si diffonde la notizia è priva di un reale contenuto; e proprio per questo viene giocosamente ripetuta da chi è a conoscenza del "fenomeno" (spesso generando una distinzione netta fra chi prende parte al fenomeno e chi, non avendo capito di cosa si tratta, non comprende l'importanza, spesso effettivamente nulla, di quello a cui "tutti" alludono).
In genere, un fenomeno di Internet tende a perdere visibilità con la stessa velocità con cui la acquisisce; in ogni caso, per la natura stessa della rete, tracce del "passaggio" del fenomeno tendono a restare sparse nella rete, a disposizione di chi volesse reperirle usando, per esempio, un motore di ricerca. È comunque quasi impossibile, per ovvi motivi, valutare accuratamente la popolarità assoluta di un fenomeno di Internet; molti si sviluppano in comunità specifiche e vi rimangono confinati, altri si diffondono in modi trasversali e giungono anche in contesti in cui l'origine stessa del fenomeno appare indecifrabile.
Alcuni suggeriscono che i fenomeni di Internet siano buoni esempi, o almeno buone metafore, delle dinamiche dei “memi”.

Il **meme** è una entità consistente in una informazione riconoscibile dall'intelletto, relativa alla cultura umana che è replicabile da una mente o un supporto simbolico di memoria, per esempio un libro, ad un'altra mente o supporto. In termini più specifici, un meme sarebbe "un'unità auto-propagantesi" di evoluzione culturale, analoga a ciò che il gene è per la genetica quindi un elemento di una cultura o civiltà trasmesso da mezzi non genetici, soprattutto per imitazione.
Il concetto ha origine, nell'ambito di una visione biologico-evoluzionistica umana, all'interno del libro di Richard Dawkins Il gene egoista del 1976, tuttavia un concetto simile era già stato formulato da William S. Burroughs nel 1962.
L'ipotesi di Dawkins è nata in ambito genetico, ricalcando l'approccio della genetica moderna, neodarwinista, all'evoluzione della vita, per ereditarietà, mutazione e selezione del “più adatto”, ed ha avuto buona fortuna, soprattutto mediatica, nel mondo scientifico non specializzato in studi sulla cultura. Tuttavia il concetto di meme è stato accolto abbastanza freddamente nelle scienze che si occupano specificamente della cultura e della sua trasmissione e modificazione (scienze socioantropologiche, cultural studies, folkloristica, ecc.).
Nel suo libro Il gene egoista, l'etologo Richard Dawkins ha introdotto il termine meme per descrivere una unità base dell'evoluzione culturale umana analoga al gene, unità base dell'evoluzione biologica, in base all'idea che il meccanismo di replica, mutazione e selezione si verifichi anche in ambitoculturale. Così come in biologia, la presenza di questi elementi, porta all'emergere spontaneo di effetti evolutivi, anche se per i memi questi si manifestano in senso diverso rispetto a quello biologico. Nel libro, Dawkins descrive il meme come una unità di informazione residente nel cervello. Si tratta di uno schema che può influenzare l'ambiente in cui si trova (attraverso l'azione degli uomini che lo portano) e si può propagare (attraverso la trasmissione culturale). Questa definizione ha creato un grande dibattito tra sociologi, biologi e scienziati di altre discipline, perché Dawkins non ha dato una spiegazione sufficiente di come la replica di unità di informazione nel cervello controlli il comportamento umano e, alla fine, la cultura. A causa di ciò, il termine "unità di informazione" è stato definito in molti modi diversi da scienziati diversi. A quasi trent'anni di distanza il dibattito è ancora in corso sul valore della memetica come disciplina scientifica. Il dibattito è stato recentemente ravvivato dalla pubblicazione del libro La macchina dei memi (1999) di Susan Blackmore in cui introduce il concetto generalizzato di replicatore, liberando così l'analogia con la genetica da vincoli eccessivi.

4Chan

4chan è un sito imageboard in lingua inglese.
Lanciato il 1º ottobre 2003, le sue bacheche vengono utilizzate principalmente per la pubblicazione di immagini e la discussione di manga e anime. Gli utenti generalmente possono postare in forma anonima ed il sito è stato associato a diverse subculture internet ed in particolare al progetto Chanology.
Gli utenti di 4chan sono anche responsabili per aver fatto nascere numerosi fenomeni di internet come lolcat, Rickrolling, Pedobeare molti altri. La bacheca "Random" è la più celebre e popolare caratteristica del sito. Conosciuta anche come "/b/", è caratterizzata dalla scarsissima regolamentazione sui contenuti pubblicabili. Gawker ha scherzosamente dichiarato che "leggere /b/ può sciogliere il cervello".
Il sito e soprattutto la sua comunità anonima ha spesso attirato su di sé l'attenzione dei mass media. Per i progettisti, 4chan è "un'ulteriore prova che la creatività è ovunque, ed i nuovi media sono meno accessibili alle agenzie pubblicitarie".The Guardian ha descritto la comunità di 4chan come "pazza, giovanile... brillante, ridicola ed allarmante."

Progetto Chanology

(anche chiamato operazione Chanology) è il nome di un movimento di protesta contro le pratiche della Chiesa di Scientology. Il progetto è nato in risposta ai tentativi della chiesa di Scientology di rimuovere da internet del materiale proveniente da una pubblicizzatissima intervista rilasciata da un membro di Scientology, l'attore Tom Cruise nel gennaio 2008.
Il progetto è stato lanciato pubblicamente in forma di un video pubblicato su YouTube, "Messaggio a Scientology", il 21 gennaio 2008. Il video affermava che il gruppo Anonymous vedeva le azioni di Scientology come una forma di censura, ed affermava l'intenzione del gruppo di "espellere la chiesa da Internet". Questo messaggio è stato seguito da una serie di attacchi DoS distribuiti, ed in seguito, fax in bianco, scherzi telefonici e altre misure destinate a disturbare le operazioni della Chiesa di Scientology. Nel febbraio 2008, i metodi della protesta sono diventati legali: il progetto Chanology ha iniziato a protestare utilizzano manifestazioni non violente e tentando di coinvolgere l'Internal Revenue Service affinché indagasse la situazione fiscale della Chiesa di Scientology negli Stati Uniti.
Le reazioni dalla Chiesa di Scientology in merito agli interventi dei manifestanti sono state varie. Inizialmente un portavoce di Scientology ha dichiarato che i membri del gruppo Anonymous "sono in possesso di alcune informazioni sbagliate" su Scientology. Un altro membro della Chiesa di Scientology ha fatto riferimento al gruppo Anonymous con l'appellativo "computer geek" ("fanatici del computer"). Più tardi, la Chiesa di Scientology ha iniziato a far riferimento al gruppo Anonymous come a dei "cyberterroristi" che perpetrano "crimini di odio religioso" contro la Chiesa.
I detrattori di Scientology hanno criticato le azioni del Progetto Chanology, affermando che si limitano a fornire alla Chiesa di Scientology la possibilità di "giocare la carta della persecuzione religiosa". Altri critici, come Mark Bunker e Tory Christman, inizialmente hanno contestato la legittimità del Progetto Chanology ed i suoi metodi, ma in seguito si sono pronunciati a sostegno del progetto nel momento in cui questo si è spostato su proteste nonviolente ed altri metodi di protesta legali.